

Department of the Interior IT Security Program

FireCode System (MA) Privacy Impact Assessment (PIA)

Version 1.01



FIR-CAM-PIA-V1.01.00-03049-02162005

**U.S. Department of the Interior
Office of the Chief Information Officer**

February 16, 2005

Prepared for:
Departmental IT Security Manager
Office of the Chief Information Officer
U.S. Department of the Interior
1849 C Street, N.W.
Washington, D.C. 20240

***Property of the United States Government
This Document Contains Sensitive But Unclassified Information***

Do not remove this notice

*Subject to Non-Disclosure - Category 3, Non-Public Information
Properly destroy in accordance with the GRS/BLM Combined Records Schedule (MS-1220, Appendix 2)*

Revision/Change Record

Revision	Date	Authorization (Optional)	Revision/Change Description	Pages Affected
V1.00			Initial Release	All
V1.01	2/16/2005	SS	Update CM number, Date	

Table of Contents

REVISION/CHANGE RECORD.....	I
SYSTEM IDENTIFICATION.....	1
SYSTEM NAME:	1
ACRONYM/ABBREVIATION:	1
ASCADS	ERROR! BOOKMARK NOT DEFINED.
ORGANIZATIONAL RESPONSIBILITY	1
A. CONTACT INFORMATION:	2
1) WHO IS THE PERSON COMPLETING THIS DOCUMENT?	2
2) WHO IS THE SYSTEM OWNER?	2
3) WHO IS THE SYSTEM MANAGER FOR THIS SYSTEM OR APPLICATION?	2
4) WHO IS THE IT SECURITY MANAGER?	2
B. SYSTEM APPLICATION/GENERAL INFORMATION	4
1) DOES THIS SYSTEM CONTAIN ANY PERSONAL INFORMATION ABOUT INDIVIDUALS?	4
2) WHAT IS THE PURPOSE OF THE SYSTEM/APPLICATION?	4
3) WHAT LEGAL AUTHORITY AUTHORIZES THE PURCHASE OR DEVELOPMENT OF THIS SYSTEM/APPLICATION?	4
C. DATA IN THE SYSTEM:	5
1) WHAT CATEGORIES OF INDIVIDUALS ARE COVERED IN THE SYSTEM?	5
2) WHAT ARE THE SOURCES OF THE INFORMATION IN THE SYSTEM?	5
a. <i>Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?</i>	5
3) ACCURACY, TIMELINESS, AND RELIABILITY	5
a. <i>How will data collected from sources other than DOI records be verified for accuracy?</i>	5
b. <i>How will data be checked for completeness?</i>	5
c. <i>Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).</i>	5
d. <i>Are the data elements described in detail and documented? If yes, what is the name of the document?</i>	5
D. ATTRIBUTES OF THE DATA	6
1) IS THE USE OF THE DATA BOTH RELEVANT AND NECESSARY TO THE PURPOSE FOR WHICH THE SYSTEM IS BEING DESIGNED?	6
2) WILL THE SYSTEM DERIVE NEW DATA OR CREATE PREVIOUSLY UNAVAILABLE DATA ABOUT AN INDIVIDUAL THROUGH AGGREGATION FROM THE INFORMATION COLLECTED, AND HOW WILL THIS BE MAINTAINED AND FILED?	6
3) WILL THE NEW DATA BE PLACED IN THE INDIVIDUAL’S RECORD?	6

4)	CAN THE SYSTEM MAKE DETERMINATIONS ABOUT EMPLOYEES/PUBLIC THAT WOULD NOT BE POSSIBLE WITHOUT THE NEW DATA?	6
5)	HOW WILL THE NEW DATA BE VERIFIED FOR RELEVANCE AND ACCURACY?	6
6)	IF THE DATA IS BEING CONSOLIDATED, WHAT CONTROLS ARE IN PLACE TO PROTECT THE DATA FROM UNAUTHORIZED ACCESS OR USE?	6
7)	IF PROCESSES ARE BEING CONSOLIDATED, ARE THE PROPER CONTROLS REMAINING IN PLACE TO PROTECT THE DATA AND PREVENT UNAUTHORIZED ACCESS?	6
8)	HOW WILL THE DATA BE RETRIEVED? DOES A PERSONAL IDENTIFIER RETRIEVE THE DATA? IF YES, EXPLAIN AND LIST THE IDENTIFIERS THAT WILL BE USED TO RETRIEVE INFORMATION ON THE INDIVIDUAL.	6
9)	WHAT KINDS OF REPORTS CAN BE PRODUCED ON INDIVIDUALS? WHAT WILL BE THE USE OF THESE REPORTS? WHO WILL HAVE ACCESS TO THEM?	7
E.	MAINTENANCE AND ADMINISTRATIVE CONTROLS	8
1)	IF THE SYSTEM IS OPERATED IN MORE THAN ONE SITE, HOW WILL CONSISTENT USE OF THE SYSTEM AND DATA BE MAINTAINED IN ALL SITES?	8
2)	WHAT ARE THE RETENTION PERIODS OF DATA IN THIS SYSTEM?	8
3)	WHAT ARE THE PROCEDURES FOR DISPOSITION OF THE DATA AT THE END OF THE RETENTION PERIOD? HOW LONG WILL THE REPORTS PRODUCED BE KEPT? WHERE ARE THE PROCEDURES DOCUMENTED?	8
4)	IS THE SYSTEM USING TECHNOLOGIES IN WAYS THAT THE DOI HAS NOT PREVIOUSLY EMPLOYED (E.G., MONITORING SOFTWARE, SMART CARDS, CALLER-ID)?	8
5)	HOW DOES THE USE OF THIS TECHNOLOGY AFFECT PUBLIC/EMPLOYEE PRIVACY?	8
6)	WILL THIS SYSTEM PROVIDE THE CAPABILITY TO IDENTIFY, LOCATE, AND MONITOR INDIVIDUALS? IF YES, EXPLAIN.	8
7)	WHAT KINDS OF INFORMATION ARE COLLECTED AS A FUNCTION OF THE MONITORING OF INDIVIDUALS?	8
8)	WHAT CONTROLS WILL BE USED TO PREVENT UNAUTHORIZED MONITORING?	8
9)	UNDER WHICH PRIVACY ACT SYSTEMS OF RECORDS NOTICE DOES THE SYSTEM OPERATE? PROVIDE NUMBER AND NAME.	8
10)	IF THE SYSTEM IS BEING MODIFIED, WILL THE PRIVACY ACT SYSTEM OF RECORDS NOTICE REQUIRE AMENDMENT OR REVISION? EXPLAIN.	9
F.	ACCESS TO DATA	10
1)	WHO WILL HAVE ACCESS TO THE DATA IN THE SYSTEM? (E.G., CONTRACTORS, USERS, MANAGERS, SYSTEM ADMINISTRATORS, DEVELOPERS, TRIBES, OTHER)	10
2)	HOW IS ACCESS TO THE DATA BY A USER DETERMINED? ARE CRITERIA, PROCEDURES, CONTROLS, AND RESPONSIBILITIES REGARDING ACCESS DOCUMENTED?	10
3)	WILL USERS HAVE ACCESS TO ALL DATA ON THE SYSTEM OR WILL THE USER’S ACCESS BE RESTRICTED? EXPLAIN.	10
4)	WHAT CONTROLS ARE IN PLACE TO PREVENT THE MISUSE (E.G., UNAUTHORIZED BROWSING) OF DATA BY THOSE HAVING ACCESS?	10
5)	ARE CONTRACTORS INVOLVED WITH THE DESIGN AND DEVELOPMENT OF THE SYSTEM AND WILL THEY BE INVOLVED WITH THE MAINTENANCE OF THE SYSTEM? IF YES, WERE PRIVACY ACT	

CONTRACT CLAUSES INSERTED IN THEIR CONTRACTS AND OTHER REGULATORY MEASURES
ADDRESSED?..... 10

6) DO OTHER SYSTEMS SHARE DATA OR HAVE ACCESS TO THE DATA IN THE SYSTEM? IF YES,
EXPLAIN..... 10

7) WHO WILL BE RESPONSIBLE FOR PROTECTING THE PRIVACY RIGHTS OF THE PUBLIC AND
EMPLOYEES AFFECTED BY THE INTERFACE?..... 10

8) WILL OTHER AGENCIES SHARE DATA OR HAVE ACCESS TO THE DATA IN THIS SYSTEM
(FEDERAL, STATE, LOCAL, OTHER (E.G., TRIBAL))?..... 10

9) HOW WILL THE DATA BE USED BY THE OTHER AGENCY?..... 10

10) WHO IS RESPONSIBLE FOR ASSURING PROPER USE OF THE DATA? 11

SYSTEM IDENTIFICATION

System Name:

FireCode System

Acronym/Abbreviation:

FireCode

Organizational Responsibility

The following organization has overall responsibility for the operation, maintenance and security for the FireCode system:

Department of the Interior, Bureau of Land Management
Office of Fire and Aviation
National Interagency Fire Center (NIFC)
3833 S. Development Avenue
Boise, ID 83705-5354
208-387-5446

A. CONTACT INFORMATION:

1) Who is the person completing this document?

Northrop Grumman Systems

2) Who are the system owners?

Corbin Newman National Fire Plan Coordinator USDA Forest Service National Fire Plan Office 201 14th Street, SW National Fire Plan 1, NW Washington DC 20024 Phone: 202-205-1332 Email: cnewman@us.fed.us	Scott Dalzell, Acting Director Ofc of Wildland Fire Coordination DOI, Office of the Secretary 1849 C Street, NW, MS 3060-MIB Washington, DC 20240 Phone: 202-606-3211 Email: Scott_Dalzell@ios.doi.gov
--	--

3) Who is the system manager for this system or application?

Elyse Turkeltaub
Fire IT Program Manager
Office of Wildland Fire Coordination
1849 C Street, NW
MS 3060-MIB
Washington, DC 20240
Phone: 202-606-0518
Fax: 202-606-3150
Email: Elyse_Turkeltaub@ios.doi.gov

4) Who is the IT Security Manager?

Don Lee, IT Security/Configuration Manager
3833 South Development Avenue
Boise, Idaho 83705-5354
208-387-5747
Don_Lee@blm.gov

5) Who is the Bureau/Office Privacy Act Officer who reviewed this document?

Sue Ellen Sloca
NBC Privacy Act Officer

1849 C Street, NW, 1415-MIB
Washington, DC 20240
Phone: 202-208-6045
Email: Sue_Ellen_Sloca@nbc.gov

6) Who is the Reviewing Official?

Robert L. Scheibel
OS/NBC Chief Information Officer
7301 W. Mansfield Ave., D-2100
Denver, CO 80235-2230
Phone: 303-969-7205
Email: Robert_L_Scheibel@nbc.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION

1) Does this system contain any personal information about individuals?

No.

a. Is this information identifiable to the individual?

Not Applicable. There is no personal information on the system.

b. Is the information about individual members of the public?

Not Applicable. There is no personal information on the system.

c. Is the information about employees?

Not Applicable. There is no personal information on the system.

2) What is the purpose of the system/application?

This is a web-based application accessible through user IDs and passwords. The database stores geospatial coordinates, names of fires, a four character code to identify the individual fire, identifiers representing Government organizational names, and the user ID and date/time stamp of the person who initially entered the data and the last modification of data.

3) What legal authority authorizes the purchase or development of this system/application?

Not Applicable. There is no personal information on the system.

C. DATA IN THE SYSTEM:

1) What categories of individuals are covered in the system?

Not Applicable. There is no personal information on the system.

2) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Not Applicable. There is no personal information on the system.

b. What Federal agencies are providing data for use in the system?

Not Applicable. There is no personal information on the system.

c. What Tribal, State and local agencies are providing data for use in the system?

Not Applicable. There is no personal information on the system.

d. From what other third party sources will data be collected?

Not Applicable. There is no personal information on the system.

e. What information will be collected from the employee and the public?

Not Applicable. There is no personal information on the system.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOI records be verified for accuracy?

Not Applicable. There is no personal information on the system.

b. How will data be checked for completeness?

Not Applicable. There is no personal information on the system.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Not Applicable. There is no personal information on the system.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

Not Applicable. There is no personal information on the system.

D. ATTRIBUTES OF THE DATA

- 1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Not Applicable. There is no personal information on the system.

- 2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

Not Applicable. There is no personal information on the system.

- 3) Will the new data be placed in the individual's record?**

Not Applicable. There is no personal information on the system.

- 4) Can the system make determinations about employees/public that would not be possible without the new data?**

Not Applicable. There is no personal information on the system.

- 5) How will the new data be verified for relevance and accuracy?**

Not Applicable. There is no personal information on the system.

- 6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

Not Applicable. There is no personal information on the system.

- 7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?**

Not Applicable. There is no personal information on the system.

- 8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

Not Applicable. There is no personal information on the system.

- 9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

Not Applicable. There is no personal information on the system.

- 10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)?**

Not Applicable. There is no personal information on the system.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS

- 1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

Not Applicable. There is no personal information on the system.

- 2) **What are the retention periods of data in this system?**

Not Applicable. There is no personal information on the system.

- 3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

Not Applicable. There is no personal information on the system.

- 4) **Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

Not Applicable. There is no personal information on the system.

- 5) **How does the use of this technology affect public/employee privacy?**

Not Applicable. There is no personal information on the system.

- 6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

Not Applicable. There is no personal information on the system.

- 7) **What kinds of information are collected as a function of the monitoring of individuals?**

Not Applicable. There is no personal information on the system.

- 8) **What controls will be used to prevent unauthorized monitoring?**

Not Applicable. There is no personal information on the system.

- 9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

Not Applicable. There is no personal information on the system.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

Not Applicable. There is no personal information on the system.

F. ACCESS TO DATA

- 1) **Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)**

Not Applicable. There is no personal information on the system.

- 2) **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Not Applicable. There is no personal information on the system.

- 3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

Not Applicable. There is no personal information on the system.

- 4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?**

Not Applicable. There is no personal information on the system.

- 5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

Not Applicable. There is no personal information on the system.

- 6) **Do other systems share data or have access to the data in the system? If yes, explain.**

Not Applicable. There is no personal information on the system.

- 7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

Not Applicable. There is no personal information on the system.

- 8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**

Not Applicable. There is no personal information on the system.

- 9) **How will the data be used by the other agency?**

Not Applicable. There is no personal information on the system.

10) Who is responsible for assuring proper use of the data?

Not Applicable. There is no personal information on the system.

The Following Officials Have Approved this Document

1) System Owner

_____ (Signature) _____ (Date)

**Name: Elyse Turkeltaub, Fire IT Program Manager
Office of Wildland Fire Coordination**

2) System Manager

_____ (Signature) _____ (Date)

**Name: Elyse Turkeltaub
Title: Fire IT Program Manager**

3) IT Security Manager

_____ (Signature) _____ (Date)

**Name: Mary H. Macleod
Title: IT Security Manager**

4) Privacy Act Officer

_____ (Signature) _____ (Date)

**Name: Sue Ellen Sloca
Title: Privacy Act Officer**

5) Reviewing Official

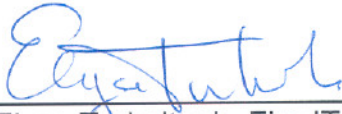
_____ (Signature) _____ (Date)

Name: Robert L. Scheibel

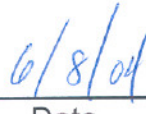
Title: Chief Information Officer

The Following Officials Have Approved this Document

1) **System Manager**

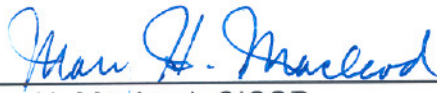


Elyse Turkeltaub, Fire IT Program Manager
Office of Wildland Fire Coordination



Date

2) **IT Security Manager**

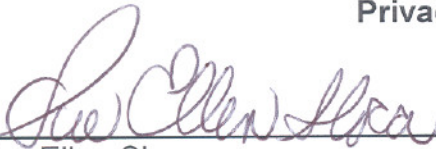


Mary H. Macleod, CISSP
National Business Center
IT Security Manager (BITSM)

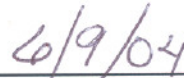


Date

3) **Privacy Act Officer**



Sue Ellen Sloca
National Business Center
Privacy Act Officer



Date

4) **Reviewing Official**



Robert L. Scheibel
National Business Center
Chief Information Officer



Date